IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

DuWayne Baird individually and on behalf of all other similarly situated individuals, Plaintiff, v. Capital One Financial Corporation, Capital One, N.A. and Capital One Bank (USA) Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED** **INJUNCTIVE RELIEF DEMANDED**

Plaintiff DuWayne Baird ("Plaintiff"), individually and on behalf of all others similarly situated, allege upon personal knowledge of the facts respectively pertaining to their own actions, and upon information and belief as to all other matters, by and through their undersigned counsel, hereby bring this Class Action Complaint against Defendant, Capital One Financial Corporation and its two primary subsidiaries Capital One, N.A. and Capital One Bank (USA) (collectively, "Capital One").

NATURE OF ACTION

1. Plaintiff asserts this class action against Capital One for its failure to exercise reasonable care in securing and safeguarding consumers' sensitive personal information, including the names, addresses, phone numbers, dates of birth, credit scores, credit limits, account balances, payment histories, social security numbers, and bank account numbers (collectively, "PII").

2. On July 29, 2019, Capital One announced that on "July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information [i.e., PII] relating to people who had applied for its credit card products and to Capital

One credit card customers."[1] The United States Federal Bureau of Investigations ("FBI") related that an individual accessed the PII by exploiting one of Capital One's misconfigured firewalls, which allowed her to access a Capital One cloud repository and exfiltrate the PII of approximately 100 million consumers in or around March 2019 (the "Data Breach").[2]

3. The hacker, known as Paige A. Thompson, who used the handle "erratic," posted the PII of these approximate 100 million consumers to her GitHub account on April 21, 2019, which was free and available for any user on the internet to download and further exploit.[3]

4. In addition to Capital One's failure to prevent the Data Breach, Capital One also failed to detect the breach for approximately three months. Upon information and belief, the posted PII of approximately 100 million consumers on Thompson's GitHub account remained exposed until at least July 17, 2019, when an unidentified tipster informed Capital One of the posting by emailing the bank's responsible disclosure address with a brief warning and a link to the GitHub address.[4]

5. The Data Breach was the result of Capital One's inadequate approach to data security and protection of PII that it collected during the course of its business. The deficiencies in Capital One's data security were so significant that the misconfigured firewall permitted access to any consumer or small business that applied for one of Capital One's credit card products from

---

1 *Overview – Frequently Asked Questions*, Capital One, (July 29, 2019), Available at https://www.capitalone.com/facts2019/ (hereinafter the "Breach Notification").

2 Harrer, Andrew, *The Alleged Capital One Hacker Didn't Cover Her Tracks*, Wired (July 29, 2019). Available at https://www.wired.com/story/capital-one-hack-credit-card-application-data/.

3 *Id.*

4 *Id.*

2005 through early 2019—approximately fourteen years of data left unprotected and exposed for any malicious actor to access, download, and exploit.[5]

6. Capital One disregarded the rights of Plaintiff and the Class (defined below) by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected; failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard customer PII; failing to take available steps to detect and prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and the Class prompt and accurate notice of the Data Breach.

7. As a result of Capital One's Data Breach, Plaintiff's and Class members' PII have definitively been exposed to criminals for misuse. The injuries Plaintiff and the Class suffered as a direct result of the Data Breach include:

i. theft of personal and financial information;

ii. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

iii. damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach, including but not limited to foregoing cash back rewards;

iv. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed

[5] Breach Notification, *supra* n.1.

bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

v. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, including, but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

vi. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by PII being exposed for theft and sale on the dark web;

vii. damages to and diminution in value of PII entrusted to Capital One for the sole purpose of purchasing products and services from Capital One; and

viii. the loss of Plaintiff's and Class members' privacy.

8. The injuries Plaintiff and the Class suffered were directly and proximately caused by Capital One's failure to implement or maintain adequate data security measures for SPI.

9. Plaintiff and the Class retain a significant interest in ensuring that their PII, which remain in Capital One's possession, are protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose PII was stolen.

10. Plaintiff, individually and on behalf of similarly situated consumers, seek to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

11. Plaintiff DuWayne Baird is a citizen of Ohio.

12. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business located at 1680 Capital One Drive, McLean, Virginia. It offers a broad spectrum of financial products and services to consumers including credit cards and is among the biggest banks in the United States with $373.6 billion in total assets as of 2019. Capital One Financial Corp. operates through its two primary subsidiaries Capital One Bank (USA) and Capital One, N.A.

13. Capital One Bank (USA), National Association is one of Capital One Financial Corporation's two principal subsidiaries. It offers a variety of credit and debit card products to consumers.

14. Capital One, National Association is one of Capital One Financial Corporation's two principal subsidiaries. It offers a broad spectrum of banking products and financial services to consumers small businesses and commercial clients.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there

are 100 or more members of the Class, pursuant to Capital One's admission that approximately 100,000,000 consumers were affected by the Data Breach.

16. This Court has personal jurisdiction over Capital One because its principal place of business is in the Eastern District of Virginia, and Capital One is authorized to and regularly conducts business in the Eastern District of Virginia.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Capital One is a corporation, has its principal place of business in this District, and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

A. The Banking System is a Constant Target for Malicious Actors

18. Data breaches have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, representing a record high and a forty percent increase from the previous year. [6] In 2017 a new record high of 1,579 breaches was reached representing a 44.7% increase over 2016.[7] The banking sector remained a high target among cyber criminals with 135 data breaches in 2018 alone.[8]

19. "The risk of cyberattack on financial services firms cannot be overstated" as financial services companies "fall victim to cybersecurity attacks 300 times more frequently than

---

[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at* https://www.idtheftcenter.org/surveys-studys/ (last visited January 23, 2019).

[7] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/ (last visited January 23, 2019).

[8] Identity Theft Resource Center, End of Year Data Breach Report (2018). Available at https://www.idtheftcenter.org/2018-data-breaches/.

businesses in other industries."[9] Indeed, "financial institutions have long been a lucrative target for cybercriminals because of the massive volumes of data and money that can be stolen."[10] A recent study from the cybersecurity firm Intsights confirmed that the Banking and Financial sectors were hit with a constant stream of cyber-attacks when compared to other sectors.[11]

20. The consequences to affected consumers are significant as sensitive personal and financial information is exposed. It is further exacerbated when, as here, compromised PII includes Social Security numbers which make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[12] Each of these fraudulent activities is difficult to detect and may not be uncovered until the number has been used in a fraudulent transaction. Moreover, it is no easy task to change or cancel a stolen Social Security number. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

---

[9] Forbes, *Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions*, August 28, 2018. Available at https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#3b3eee36e906.

[10] Help Net Security, *Increasing number of financial institutions falling prey to cyber Attacks*, November 9, 2016. Available at https://www.helpnetsecurity.com/2016/11/09/financial-institutions-cyber-attacks/.

[11] CISO MAG, Banking and Financial sectors are prime target for hackers, May 3, 2019 https://www.cisomag.com/banking-and-financial-sectors-are-prime-target-for-hackers-survey/ (last visited July 30, 2019).

[12] The United States Government Accountability Office explained that theft involving social security numbers is the most insidious not only because it often takes time for the victim to become aware of the theft, but that as a result they will often face "substantial costs and inconveniences repairing damage to their credit records…[and their] good name." Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO (June 2007), available at https://www.gao.gov/new.items/d07737.pdf (the "GAO Report")(last visited March 21, 2019).

[13] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited February 13, 2019).

21. Capital One knew the importance of safeguarding patient PII entrusted to it and of the foreseeable consequences if its data security systems were to be breached, including the significant costs that would be imposed on its customers as a result of a breach.

B. Plaintiff's Transaction with Capital One

22. In or about December 2011, Plaintiff Baird applied for a credit card with Capital One.

23. Since the announcement of the Data Breach, Plaintiff Baird continues to monitor his accounts in an effort to detected and prevent any misuses of his personal information.

24. Plaintiff Baird has, and continues to, spend his valuable time to protect the integrity of his finances and credit – time which she would not have had to expend but for the Data Breach.

25. Plaintiff Baird would not have applied for a credit card with and provided PII to Capital One during the period of the Data Breach had Capital One disclosed that it lacked adequate computer systems and data security practices to safeguard consumers' PII from theft.

26. Plaintiff suffered actual injury from having his PII stolen as a result of the Data Breach.

27. Plaintiff Baird suffered actual injury and damages in paying money to, and purchasing products through, Capital One's business during the Data Breach (e.g., paying interest on credit cards, paying minimum balance fees, and other banking fees), expenditures which he would not have made with Capital One had Capital One disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII from theft.

28. Plaintiff Baird suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that the Plaintiff entrusted to Capital One for

the purpose of applying for and using Capital One's products, which was compromised in and as a result of the Data Breach.

29. Plaintiff Baird suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and has concerns for the loss of his privacy.

30. Plaintiff Baird has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

31. Plaintiff Baird has a continuing interest in ensuring his PII, which remains in the possession of Capital One, is protected and safeguarded from future breaches.

C. Capital One's Customer Data Collection Practices

32. Capital One is a for-profit corporation and one of the largest banking institutions in the United States.

33. As part of applying for a credit card and other financial services, consumers provide banks their names, addresses, social security numbers, and other valuable, sensitive, and private PII.

34. At all relevant times, Capital One was well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored from the applications is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

35. Banking repositories and databases are popular targets for cyberattacks, especially given the extremely sensitive nature of the PII stored on those repositories and databases. The frequency and prevalence of attacks make it imperative that banks such as Capital One routinely monitor for exploits and cyberattacks and regularly update their software and security procedures.

36. Such exploits can go undetected for a long period of time, especially if industry best practices are not routinely used.

37. PII is a valuable commodity. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal, private information on multiple underground Internet websites. PII is valuable to identity thieves because they can use victims' personal data—including PII—to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, and credit cards.

38. This is especially true for banks, given that the PII disclosed in this Data Breach was precisely the PII Capital One requested to process and, in some cases, approve consumers for credit cards and other banking products.

39. Legitimate organizations and the criminal underground alike recognize the value of PII contained in a data systems; otherwise, the latter would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[14]

40. Professionals tasked with trying to stop fraud and other misuse know that PII have real monetary value in part because criminals continue their efforts to obtain this data.[15] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one

---

[14] Verizon 2014 PCI Compliance Report, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54.

[15] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, *CIO Magazine* (October 2016), http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,579 data breaches in 2017, which represents a 44.7 percent increase over the record high figures reported for 2016.[16]

41. The PII of consumers remains of high value to identity criminals, as evidenced by the prices criminals will pay through black-market sources, or what is often called the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a complete set of bank account credentials can fetch a thousand dollars or more (depending on the associated credit score or balance available to criminals).[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. [18]

42. At all relevant times, Capital One knew, or reasonably should have known, of the importance of safeguarding PII, and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

43. Capital One was, or should have been, fully aware of the significant volume of daily online credit applications, amounting to tens of thousands of daily interactions with consumers' PII, and thus, the significant number of individuals who would be harmed by a breach of Capital One's systems.

---

[16] *2017 Annual Data Breach Year-End Review,* IDTheftCenter (2017), https://www.idtheftcenter.org/2017-data-breaches.

[17] *Here's How Much Thieves Make By Selling Your Personal Data Online, Business Insider,* http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, May 27, 2015.

[18] *Here's How Much Your Personal Information Is Selling for on the Dark Web* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

44. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, such as banking institutions, retailers, and restaurant chains, Capital One's approach to maintaining the privacy and security of Plaintiff's and Class members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

D. The Capital One Data Breach

45. On July 29, 2019, Capital One admitted to one of the largest data breaches in history, in which more than 100 million US consumers were affected.[19] The Data Breach notice stated in relevant part:

> Capital One Announces Data Security Incident
>
> * * *
>
> MCLEAN, Va., July 29, 2019 /PRNewswire/ -- Capital One Financial Corporation (NYSE: COF) announced today that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.
>
> * * *
>
> Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.
>
> * * *
>
> The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:
>
> - Customer status data, e.g., credit scores, credit limits, balances, payment

[19] Breach Notification, *supra* n.1.

history, contact information

- Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018.

* * *

- About 140,000 Social Security numbers of our credit card customers
- About 80,000 linked bank account numbers of our secured credit card customers

* * *

We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.

Safeguarding our customers' information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.

For more information about this incident and what Capital One is doing to respond, visit www.capitalone.com/facts2019. In Canada, information can be found at www.capitalone.ca/facts2019 and www.capitalone.ca/facts2019/fr. The investigation is ongoing and analysis is subject to change. As we learn more, we will update these websites to provide additional information. [20]

46. The Capital One Data Breach occurred because Capital One failed to secure the PII of approximately 100 million consumers in Capital One's cloud-based repository and database.[21]

47. Capital One also reported that the Data Breach impacted consumers who applied for Capital One credit card products from 2005 through "early 2019," with information that included "personal information Capital One routinely collects at the time it receives credit card

[20]Capital One Announces Data Security Incident ("Security Incident"), Available at http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle_pf&ID=2405043

[21] Breach Notification, *supra* n.1.

applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income."[22]

48. In addition to the aforementioned "routine" collections, Capital One also admitted consumers' credit scores, credit limits, balances, payment histories, contact information, and "fragments of transaction data from a total of 23 days during 2016, 2017 and 2018."[23]

49. Capital One further admitted that "about 140,000 Social Security numbers of [its] credit card customers" and "about 80,000 linked bank account numbers of our secured credit card customers" were also disclosed in the Data Breach.[24]

50. At no point did Capital One offer any concrete assistance or offer to remunerate Plaintiff or the Class for its negligence. Despite acknowledging that the PII was stolen by a malicious actor and placed on the Internet for anyone to access, download, and use, Capital One attempted to downplay the gravity of breach claiming " it is unlikely that the information was used for fraud or disseminated by this individual."[25]

51. This PII was compromised due to Capital One's acts and omissions and its failure to properly protect the PII, despite being aware of cybersecurity standards, industry best practices, and the vulnerability of financial service institutions to attack. See e.g. Equifax.[26]

52. In addition to its failure to prevent the Data Breach, Capital One also failed to detect the breach for at least three months—despite it being publicly represented on the popular and often

---

[22] Breach Notification, *supra* n.1.
[23] Breach Notification, *supra* n.1.
[24] Breach Notification, *supra* n.1.
[25] Security Incident, *supra* n.20.
[26] 2017 Cybersecurity Incident & Important Consumer Information. Available at https://www.equifaxsecurity2017.com/consumer-notice/.

trafficked GitHub website.[27] Intruders, therefore, had at least three months to access, collect, download, and make use of this information for fraudulent and other malicious purposes.

53. During this time, Capital One failed to recognize its systems had been breached and that intruders were stealing the PII of 100 million credit card applicants. Indeed, the breach was not even discovered as a result of Capital One's diligence or their internal cyber security systems, but rather by a third party who "sent a message to the company's responsible disclosure email address with a link to the GitHub page."[28]

54. While timely action by Capital One in identifying the Breach would likely have significantly reduced the harmful consequences, instead, their inaction and negligence contributed to the scale of the Data Breach and the resulting damages to Plaintiff and Class members.

E. Defendants' Privacy Policies and Agreements to Keep PII Confidential

55. As a condition of credit, Capital One required applicants to provide them with certain personal information. In their ordinary course of business, Defendants maintained this personal information, including, but not limited to, names, addresses, dates of birth and Social Security numbers.

56. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class members' PII, Defendants assumed legal and equitable duties to those individuals. Defendants knew or should have known that they were responsible for protecting Plaintiff's and Class

---

[27] CNET, *Capital One data breach involves 100 million credit card applications*. Available at https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/ (Thompson [the hacker] allegedly posted details about the hack on a GitHub page in April, and talked about the attack on Twitter and Slack discussions, according to the FBI. The page had been up since April 21, with the IP address for a specific server containing the company's sensitive data.)

[28] *Id.*

members' PII from disclosure. At all relevant times, Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII.

57. Plaintiff and the Class members, as credit card applicants, relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

58. In addition to their obligations under the law, Capital One independently and routinely promised to safeguard PII. Examples include:

> "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[29]

> Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you…..[30]

> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.[31]

F. Capital One Failed to Comply with Federal Requirements

59. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[32]

---

[29] https://www.capitalone.com/bank/privacy/

[30] https://www.capitalone.com/identity-protection/privacy/faq

[31] https://www.capitalone.com/identity-protection/privacy/statement

[32] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

60. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[33] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

61. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[34]

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[33] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[34] FTC, *Start With Security*, *supra* note 32.

63. Capital One's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data (i.e., PII) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. In this case, Capital One was at all times fully aware of its obligation to protect the financial data—including PII—of Capital One's applicants because of its existence a one of the United States' largest financial institutions. Capital One was also aware of the significant repercussions if it failed to do so because Capital One collected applicant data from millions of consumers monthly (if not daily) and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

G. The Data Breach Caused Harm and Will Result in Additional Fraud

65. The ramifications of Defendant's failure to keep Patients' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

66. Consumer victims of data breaches are more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[35]

67. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[36] The FTC describes "identifying

[35] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

[36] 17 C.F.R § 248.201 (2013).

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[37]

68. PII are valuable commodities to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have PII, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[38]

69. Identity thieves can use PII, such as that of Plaintiff and Class members, which Capital One failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

70. Analysis of a 2016 survey of 5,028 consumers found "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[39]

71. As a result of Capital One's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class members has been driven even higher.

---

[37] *Id.*

[38] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[39] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new , February 1, 2017.

72. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the six years preceding 2016.[40]

73. Moreover, reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[41]

74. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges,[42] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

75. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent

---

[40] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point.

[41] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[42] Hadley Malcom, *Consumers Rack Up $14.3 Billion in Gray Charges, Research Study Commissioned For Billguard By Aite Research, Usa Today* (July 25, 2013), available at: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[43]

76. The victims here—Plaintiff and the Class—are no different, as they are faced with an arduous path to secure their PII in response to Capital One's negligence. Plaintiff and the Class must take at least the following steps to attempt to prevent further misuse of their PII:

a. Review and monitor credit card statements for any unusual or unknown charges;

b. Contact their financial institution (which is not necessarily Capital One) to determine if there is any suspicious activity on their accounts;

c. Change their account information;

d. Place a fraud alert on their credit bureau reports;

e. Place a security freeze on their credit bureau reports; and

f. Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

77. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

---

[43] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 19,2019).

78. There is a very strong probability that those impacted by Capital One's failure to secure their PII could be at risk of fraud and identity theft for extended periods of time.

79. Thus, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

H. Plaintiff and Class Members Suffered Damages

80. The PII of Plaintiff and Class members are private and sensitive in nature and was left inadequately protected by Capital One. Capital One did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

81. The Data Breach was a direct and proximate result of Capital One's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Capital One's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

82. Capital One had the resources to prevent a breach, but instead chose to put profit before consumers' privacy and protection of consumers' PII.

83. Had Capital One remedied the deficiencies in its computer systems, followed federal and state guidelines, and adopted security measures recommended by experts in the field,

Capital One would have prevented intrusion into its computer systems and, ultimately, the theft of its consumers' confidential PII.

84. As a result of Capital One's wrongful actions, inaction, negligent security practices, and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

85. Capital One's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class members' information on the Internet's black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their PII;

f. loss of privacy;

g. money paid to, and purchasing products from, Capital One's business during the Data Breach (e.g., paying interest on credit cards, paying minimum balance fees, and other banking fees), expenditures which Plaintiff and Class members would not have made with Capital One had Capital One disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII from theft;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

86. While Plaintiff's and Class members' PII have been stolen, Capital One continues to hold PII of consumers, including Plaintiff's and Class members' PII. Particularly because Capital One has demonstrated an inability to prevent a breach, Plaintiff and Class members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4), seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiff seeks certification:

> All persons residing in the United States who applied for Capital One credit card products from 2005 through 2019 and whose PII was disclosed to unauthorized third parties (the "Nationwide Class").

88. Additionally, Plaintiff brings this action on behalf of a state sub class action seeking damages and equitable relief on behalf of the following :

> All persons residing in the State of Ohio who applied for Capital One credit card products from 2005 through 2019 and whose PII was disclosed to unauthorized third parties (the "Ohio Sub Class").

89. Excluded from the Classes are Capital One; any parent, affiliate, or subsidiary of Capital One; any entity in which Capital One has a controlling interest; any of Capital One's officers or directors; or any successor or assign of Capital One. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

90. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

91. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the Classes are so numerous that joinder of all members is impracticable. While Plaintiff does not know the exact number of the members of the Classes, Plaintiff believes the Nationwide Class contains approximately 100 million people. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media, and/or published notice.

92. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirements, this action involves common questions of law and fact exist as to all members of the Classes, and predominate over any questions affecting individual members of the Classes. Such questions of law and fact common to the Classes include, but are not limited to:

a. Whether Capital One had a legal duty to implement and maintain reasonable and adequate security procedures and practices for the protection of information it collected and stored from consumers who applied for Capital One credit card products;

b. Whether Capital One had a duty to adequately protect PII;

c. Whether and when Capital One knew or should have known of the susceptibility of its computer systems to a data breach;

d. Whether Capital One's security measures to protect its computer systems were reasonable in light of the FTC data security recommendations and best practices recommended by data security experts;

e. Whether Capital One engaged in the wrongful conduct alleged herein;

f. Whether Capital One was negligent in failing to implement reasonable and adequate security procedures and practices to protect the information it collected and stored from consumers who applied for Capital One credit card products;

g. Whether Capital One's failure to implement adequate data security measures resulted in or was the proximate cause of the Data Breach;

h. Whether Capital One's conduct, practices, actions, and/or omissions constituted unfair or deceptive trade practices;

i. Whether Capital One's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer systems, resulting in the loss of the PII belonging to Plaintiff and Class members;

j. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Capital One's failure to reasonably protect its computer systems and data network; and

k. Whether Plaintiff and Class members are entitled to relief, including equitable relief.

93. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with rule 23(a)(3), Plaintiff's claims are typical of the claims of the members of the Classes. Plaintiff is a consumer who provided PII to in order to apply for Capital One credit card products and had their PII compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief of the Class members.

94. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the respective Classes and is committed to pursuing this matter against Capital One to obtain relief for the Classes. Plaintiff

has no conflicts of interest with either Class members. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Classes' interests. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Classes. Plaintiff's interests are coincident with, and not antagonistic to, those of the other members of the Classes.

95. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Classes are relatively small compared to the burden and expense required to individually litigate their claims against Capital One, and thus, individual litigation to redress Capital One's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

96. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Capital One, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole.

97. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues are set forth in Paragraphs [[129(a)–(k)]] above.

98. Finally, all members of the proposed Classes are readily ascertainable. Capital One has access to information regarding the applications from consumers for the span of time from 2005 through 2019 and the consumers affected by the Data Breach. Using this information, Class members can be identified and their contact information ascertained for the purpose of providing notice to the Classes.

FIRST CLAIM FOR RELIEF
Breach of Implied Contract
(On behalf of all Classes)

99. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

100. Capital One solicited and invited Plaintiff and Class members to apply for credit card products by providing their PII. Plaintiff and Class members accepted Capital One's offers and provided their PII to Capital One to apply for Capital One credit card products.

101. When Plaintiff and Class members applied Capital One credit card products, they provided their PII to Capital One. In so doing, Plaintiff and Class members on the one hand, and Capital One on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiff and Class members agreed that their PII was valid, while Capital One agreed that it would use Plaintiff's and Class members' PII in its possession for only the agreed-upon purpose of processing the credit card product application, and no other purpose.

102. Implicit in the agreement to use the PII in its possession for only the agreed-upon application and no other purpose was the obligation that Capital One would use reasonable measures to safeguard and protect the PII of Plaintiff and Class members in its possession.

103. By accepting PII for credit card product applications, Capital One assented to and confirmed its agreement to reasonably safeguard and protect Plaintiff's and Class members' PII from unauthorized disclosure or uses and to timely and accurately notify Plaintiff and Class members if their data had been breached and/or compromised.

104. Plaintiff and Class members would not have provided and entrusted their PII to Capital One to apply for the Capital One credit card products in the absence of the implied contract between them and Capital One.

105. Plaintiff and Class members fully performed their obligations under the implied contracts with Capital One.

106. Capital One breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect Plaintiff's and Class members' PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

107. Capital One breached the implied contracts it made with Plaintiff and Class members by failing to ensure that Plaintiff's and Class members' PII in its possession was used only for the agreed-upon application verification and no other purpose.

108. Plaintiff and Class members conferred a monetary benefit on Capital One which has accepted or retained that benefit. Specifically, the credit card products typically carry annual fees and other charges (e.g. interest) for use. In exchange, Plaintiff and Class members should

have received the services that were the subject of the transaction and should have been entitled to have Capital One protect their PII with adequate data security measures.

109. Capital One failed to secure Plaintiff's and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

110. Capital One acquired the PII through inequitable means when it failed to disclose the inadequate security practices previously alleged.

111. If Plaintiff and Class members had known that Capital One would employ inadequate security measures to safeguard PII, they would not have applied for the Capital One credit card products.

112. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One on the one hand, and Plaintiff and Class members on the other, Plaintiff and Class members sustained actual losses and damages as described in detail above.

113. Plaintiff and Class members were harmed as the result of Capital One's breach of the implied contracts because their PII was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class members are further damaged as their PII remains in the hands of those who obtained it without their consent.

114. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiff and Class members as described above.

SECOND CLAIM FOR RELIEF
Negligence
(On behalf of all Classes)

115. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

116. Capital One solicited and took possession of Plaintiff's and the Class members' PII, and Capital One had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Capital One further had a duty to destroy Plaintiff's and Class members' PII within an appropriate amount of time after it was no longer required by Capital One, in order to mitigate the risk of such non-essential PII being compromised in a data breach.

117. Upon accepting and storing Plaintiff's and Class members' PII in its computer systems and on its networks, Capital One undertook and owed a duty of care to Plaintiff and Class members to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII and to use commercially-reasonable methods to do so. Capital One knew that the PII was private and confidential, and should be protected as private and confidential.

118. Capital One owed a duty of care not to subject Plaintiff and Class members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

119. Capital One owed a duty of care to Plaintiff and Class members to quickly detect a data breach and to timely act on warnings about data breaches.

120. Capital One's duties arose from its relationship to Plaintiff and Class members and from industry custom.

121. Capital One, through its actions and/or failures to act, unlawfully breached duties to Plaintiff and Class members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the PII entrusted to it.

122. Capital One, through its actions and/or failures to act, allowed unmonitored and unrestricted access to unsecured PII.

123. Capital One, through its actions and/or failures to act, failed to provide adequate supervision and oversight of the PII with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiff's and Class members' PII, misuse that PII, and intentionally disclose it to unauthorized third parties without consent.

124. Capital One knew, or should have known, the risks inherent in collecting and storing PII, the importance of adequate security and the well-publicized data breaches within the financial services industry.

125. Capital One knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' PII.

126. Due to Capital One's knowledge that a breach of its systems would damage millions of its customers, including Plaintiff and Class members, Capital One had a duty to adequately protect its data systems and the PII contained thereon.

127. Capital One had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Capital One with their PII was predicated on the understanding that Capital One would take adequate security precautions to safeguard that information. Moreover, only Capital One had the ability to protect its systems and the PII stored on those systems from attack.

128. Capital One's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Capital One's misconduct included failing to: (1) secure its computer systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

129. Capital One also had independent duties under federal laws that required Capital One to reasonably safeguard Plaintiff's and Class members' PII, and promptly notify them about the Data Breach.

130. Capital One breached its duties to Plaintiff and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Customer Data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class members' PII before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

131. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused,

Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII while it was within Capital One's possession or control.

132. The law further imposes an affirmative duty on Capital One to timely disclose the unauthorized access and theft of Plaintiff's and Class members' PII, so that Plaintiff and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

133. Capital One breached its duty to notify Plaintiff and Class Members of the unauthorized access to their PII by waiting to notify Plaintiff and Class members, and then by failing to provide Plaintiff and Class members sufficient information regarding the breach.

134. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiff's and Class members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII while it was within Capital One's possession or control.

135. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Capital One prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

136. Upon information and belief, Capital One improperly and inadequately safeguarded Plaintiff's and Class members' PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Capital One's failure to take proper security measures to protect sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class members' PII.

137. Capital One's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

138. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint

139. Capital One's failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiff's and Class members' PII being accessed and stolen through the data breach.

140. Capital One breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII.

141. As a result of Capital One's breach of duties, Plaintiff and the Class suffered damages including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage

and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

THIRD CLAIM FOR RELIEF
Negligence *Per Se*
(On behalf of all Classes)

142. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

143. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Capital One, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Capital One's duty in this regard.

144. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII, and not complying with applicable industry standards, as described in detail herein. Capital One's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the immense damages that would result to Plaintiff and Class members.

145. Capital One's violation of Section 5 of the FTC Act constitutes negligence *per se*.

146. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

147. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

148. As a direct and proximate result of Capital One's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft;

damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

149. Additionally, as a direct and proximate result of Capital One's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Capital One's possession and is subject to further unauthorized disclosures so long as Capital One fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On behalf of all Classes)

150. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

151. Plaintiff and members of the Class conferred a monetary benefit on Capital One. Specifically, they provided and entrusted their PII to Capital One.

152. In exchange, Plaintiff and Class members should have been entitled to have Capital One protect their PII with adequate data security.

153. Capital One appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Capital One's conduct toward Plaintiff and Class Members as described herein; Plaintiff and Class members conferred a benefit on Capital

One and accepted or retained that benefit. Capital One used Plaintiff's and Class members' PII for business purposes.

154. Capital One failed to secure Plaintiff's and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

155. Capital One acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged, as well as failing to destroy or otherwise purge the PII from its computer systems after Capital One no longer had a legitimate business purpose to maintain that PII.

156. If Plaintiff and Class members knew that Capital One would not secure their PII using adequate security, they would not have applied for Capital One credit card products.

157. Plaintiff and Class members have no adequate remedy at law.

158. Under the circumstances, it would be unjust for Capital One to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

159. Under the principles of equity and good conscience, Capital One should not be permitted to retain the PII belonging to Plaintiff and Class members because Capital One failed to implement the data management and security measures that industry standards mandate.

160. Capital One should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Capital One should be compelled to refund the amounts that Plaintiff and Class members overpaid for security they did not receive.

FIFTH CLAIM FOR RELIEF
Breach of Confidence
(On behalf of all Classes)

161. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

162. At all times during Plaintiff's and Class Members' interactions with Defendants, Capital One was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that was provided to them.

163. As alleged herein and above, Capital One's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

164. Plaintiff and Class Members provided their respective PII to Capital One with the explicit and implicit understandings that Capital One would protect and not permit the PII to be disseminated to any unauthorized parties.

165. Plaintiff and Class Members also provided their respective PII to Capital One with the explicit and implicit understanding that Capital One would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

166. Capital One voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

167. Due to Capital One's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties in breach of Plaintiff's and Class Members' confidence, and without their express permission.

168. As a direct and proximate cause of Capital One's actions and/or omissions, Plaintiff and Class Members have suffered damages.

169. But for Capital One's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Capital One's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

170. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Capital One's unauthorized disclosure of Plaintiff's and Class Members' PII. Capital One knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Capital One failed to observe industry standard information security practices.

171. As a direct and proximate result of Capital One's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy

172. As a direct and proximate result of Capital One's breaches of confidence, Plaintiff and Class Members have suffered and will continue to incur injury and suffer economic and non-economic losses.

SIXTH CLAIM FOR RELIEF
Invasion of Privacy
(On behalf of all Classes)

173. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

174. Plaintiff and Class members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

175. Capital One owed a duty to its credit product applicant, including Plaintiff and Class members, to keep their PII confidential.

176. Defendants failed to protect and released to unknown and unauthorized third parties' databases containing the PII of Plaintiff and Class members.

177. Defendants allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class members, by way of Defendants' failure to protect the PII in the databases.

178. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class members, especially where the information includes Social Security numbers and dates of birth, is highly offensive to a reasonable person.

179. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PII to Defendants as part of their use of Defendants' services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

180. The Data Breach at the hands of Defendants constitutes an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

181. Capital One acted with a knowing state of mind when it permitted the Data Breach because it had actual knowledge that its information security practices were inadequate and insufficient.

182. As a proximate result of the above acts and omissions of Defendants, the PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

183. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PII maintained by Defendants can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

SEVENTH CLAIM FOR RELIEF
Ohio Consumer Sales Practices Act
Ohio Rev. Code §§ 1345.01, *et seq.*
(On Behalf of the Ohio Subclass)

184. Plaintiff DuWayne Baird ("Plaintiff," for purposes of this Count), individually and on behalf of the other Ohio Subclass Members, restates and reallege paragraphs 1 through 98 as if fully set forth herein

185. Capital One operating in Ohio engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.01(A) and (B), including but not limited to the following:

i. Failing to enact adequate privacy and security measures to protect the Ohio Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Capital One Data Breach;

ii. Failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Capital One Data Breach;

iii. Knowingly and fraudulently misrepresenting that it would maintain adequate data privacy and security practices and procedures to safeguard the Ohio Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

iv. Omitting, suppressing, and concealing the material fact of the inadequacy of its privacy and security protections for the Ohio Subclass Members' Personal Information;

v. Knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Ohio Subclass Members' Personal Information;

vi. Failing to maintain the privacy and security of the Ohio Subclass Members' Personal Information, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Capital One Data Breach; and

vii. Failing to disclose the Capital One Data Breach to the Ohio Subclass Members in a timely and accurate manner, in violation of the duties imposed by Ohio Rev. Code § 1349.19(B).

186. As a direct and proximate result of Capital One's practices, the Ohio Subclass Members suffered injury and/or damages, including but not limited to time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

187. The above unfair and deceptive acts and practices by Capital One were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Ohio Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

188. Capital One knew or should have known that its computer systems and data security practices were inadequate to safeguard the Ohio Subclass Members' Personal Information and that risk of a data breach or theft was high. Capital One's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

189. Pursuant to Ohio Rev. Code § 1345.09, Plaintiff and the Ohio Subclass Members seek an order enjoining Capital One's unfair and/or deceptive acts or practices, actual damages – trebled (to be proven at the time of trial), attorneys' fees and costs, and any other just and proper relief, to the extent available under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq.*

EIGHT CLAIM FOR RELIEF
Declaratory Judgment
(On behalf of Classes)

190. Plaintiff restates and realleges paragraphs 1 through 98 as if fully set forth herein.

191. As previously alleged, Plaintiff and Class members entered into an implied contract that required Capital One to provide adequate security for the PII it collected from their applications for Capital One credit card products. As previously alleged, Capital One owes duties of care to Plaintiff and Class members that require it to adequately secure PII.

192. Capital One still possesses PII pertaining to Plaintiff and Class members.

193. Capital One has not announced or otherwise notified Plaintiff and Class members that their PII are sufficiently protected or, more importantly, expunged from Capital One's servers so as to prevent any further breaches or compromises.

194. Indeed, Capital One has stated that PII from Capital One credit card product applications submitted as far back as 2005 is subject to the Data Breach.

195. Accordingly, Capital One has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that Capital One's lax approach towards data security has become public, the PII in its possession is more vulnerable than before.

196. Actual harm has arisen in the wake of the Data Breach regarding Capital One's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

197. Plaintiff, therefore, seeks a declaration that: (a) Capital One's existing data security measures do not comply with its contractual obligations and duties of care; and (b) in order to comply with its contractual obligations and duties of care, Capital One must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Capital One's systems on a periodic basis, and ordering Capital One to

promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Capital One is compromised, hackers cannot gain access to other portions of Capital One's systems;

v. purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

vi. conducting regular database scans and security checks;

vii. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

viii. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Capital One's customers should take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes, respectfully seeks from the Court the following relief:

a. Certification of the Classes as requested herein;

b. Appointment of Plaintiff as Class representative and his undersigned counsel as Class counsel;

c. Award Plaintiff and members of the proposed Class damages;

d. Award Plaintiff and members of the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Capital One's insufficient data protection practices at issue herein and Capital One's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Capital One's acts and practices with respect to the safekeeping of PII are negligent;

f. Award Plaintiff and members of the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiff and members of the proposed Class reasonable attorney fees and costs of suit, including expert witness fees; and

h. Award Plaintiff and members of the proposed Class any further relief the Court deems proper.

Dated: July 30, 2019

Respectfully submitted,

MURPHY, FALCON & MURPHY

/s/

John G. Harnishfeger (Virginia Bar No. 36878)
Attorney for Plaintiff
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Fax: (410) 539-6599
john.harnishfeger@murphyfalcon.com

/s/
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (Florida Bar No. 324681)
Ryan J. McGee (Florida Bar No. 64957)
Patrick A. Barthle (Florida Bar No.99286)
Attorneys for Plaintiff*
*pro hac vice applications pending
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
JYanchunis@ForThePeople.com
RMcGee@ForThePeople.com
PBarthle@ForThePeople.com

JURY DEMAND

Plaintiff, on behalf of himself and the Class of all others similarly situated, hereby demands a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

/s/
John G. Harnishfeger (Virginia Bar No. 36878)